2 Проблеми розвитку нормативної та методичної баз системи захисту інформації. Метрологічне забезпечення систем ТЗІ. Стандартизація, сертифікація та випробування засобів ТЗІ

УДК 681.31

АРХИТЕКТУРА СИСТЕМИ ТЕХНИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

Николай Будько, Михаил Короленко, Евгений Федченко
ОАО "КП ОТИ"

Аннотация: **На основе анализа требований к защите информации, изложенных в соответствующих законах Украины, стандартах и нормативных документах Системы технической защиты информации, авторы излагают свой взгляд на назначение и функции систем технической защиты информации, а также возможную архитектуру ее основного компонента - Подсистемы защиты информации в автоматизированной системе.**
Summary: **On the base of analysis demands to information protection, stated in the corresponding lows of Ukraine, standards and normative documents of System of technical information protection, the authors expound theirview on the appointment and functions of system of technical information protection, fnd olso possible architecture of its main component – Subsystem of technical protection futomated system.**
Ключевые слова: **техническая защита информации, архитектура системы, функции, компоненты.**

Проблемы защиты информации и создания необходимых средств для ее сбережения, обработки, хранения и распространения существуют ровно столько же лет, сколько и само понятие «информация». С ростом роли информации в обществе, в деятельности организаций, предприятий и отдельных лиц растет и стремление их конкурентов получить эту информацию и использовать ее в своих целях. При этом меняется характер средств несанкционированного получения и способов использования информации: от примитивного «подглядывания» к современным средствам и методам ведения «информационных войн». Понятно, что соответственно должны эволюционировать как виды средств и методов защиты, так и требования к их функциональным возможностям и характеристикам.

Авторами предпринята попытка на основе анализа современных требований к защите информации, изложенных в соответствующих Законах Украины, стандартах и нормативных документах Системы технической защиты информации [1-6], изложить свой взгляд на назначение и функции таких систем защиты, а также их возможную архитектуру. При этом прежде всего речь идет о защите информации от несанкционированного доступа в автоматизированных системах (АС), которые являются в какой-либо степени собственностью государства, поскольку требования к защите информации в других системах, а также к выбору необходимых для этого средств, в соответствии с Законом Украины [1], определяются собственником автоматизированной системы или информации. На наш взгляд, очень важным является вопрос унификации подходов к реализации мероприятий по обеспечению информационной безопасности, как наиболее сложному и трудоемкому компоненту, обеспечивающему безопасность информационных систем. Особую роль играет при этом правильный выбор архитектуры системы защиты, включая унифицированный набор ее компонент, их функций, способов организации взаимодействия.

Ниже предлагается архитектура комплексной Подсистемы ТЗИ, апробированная в разработках ОАО "КП ВТИ" и проходящая опытную эксплуатацию на Юго-Западной железной дороге Украины. По нашему мнению, данная архитектура может быть основой для разработки унифицированных Подсистем защиты информации в АС.

I Комплексная система ТЗИ

Системы защиты информации в автоматизированных системах, общих и корпоративных сетях предназначены для обеспечения *безопасной информационной технологии*, т. е. обеспечения доступности и конфиденциальности информации, целостности информационных и других ресурсов и обеспечения наблюдаемости.

Для предотвращения возможности реализации угроз ресурсам АС необходима разработка и использование в АС комплексной системы технической защиты информации (ТЗИ). Требования к такой системе предусматривают централизованное управление средствами и механизмами защиты на основе определенной владельцем АС политики информационной безопасности и реализующего ее плана технической защиты информации.

Комплексной системой технической защиты информации [4] принято называть совокупность организационно-правовых и инженерных мероприятий, а также программно - аппаратурных средств, которые обеспечивают ТЗИ в АС. Именно на нее нормативными документами Системы ТЗИ возлагается задача обеспечения уже упомянутых функциональных свойств защищенных АС. Эта задача решается как техническими, так и программными средствами базового и прикладного программного обеспечения, а также с использованием специально разрабатываемых программных и аппаратурных средств ТЗИ.

Организационно-правовыми мероприятиями реализуется комплекс соответствующих нормативно-правовой базе государства административных и ограничительных мер, направленных на оперативное решение задач защиты путем анализа угроз, регламентации деятельности персонала и определения порядка функционирования средств обеспечения информационной деятельности и средств ТЗИ, а также путем создания служб (или назначения администраторов ТЗИ), ответственных за их реализацию. К таким мероприятиям относятся также определение контролируемых зон и организация контроля доступа в эти зоны. Для реализации мероприятий этой группы в большинстве случаев нет необходимости использования средств, являющихся компонентами АС.

Основной задачей ***технических*** мероприятий является обеспечение физической и информационной безопасности.

Физическая безопасность достигается за счет:

- выбора инженерно-технических средств, исключающих несанкционированный доступ к объектам и техническим средствам;
- блокирования каналов утечки информации, включая использование процедур контролируемой ликвидации данных;
- блокирования несанкционированного физического доступа к активным компонентам АС (информации или ресурсам ИС), находящимся в контролируемой зоне;
- выявления электронных устройств перехвата информации;
- выбор и проверки исправности и работоспособности технических средств обеспечения информационной деятельности.

Для реализации мероприятий этой группы используются устройства, чаще всего не являющиеся элементами АС и относящиеся к достаточно автономным *первичным* техническим средствам ТЗИ (например, устройства защиты информации от утечки по каналам побочных электромагнитных излучений). Среди немногочисленных исключений – автоматизированные средства управления физическим доступом, системы охранной и пожарной сигнализации, которые могут быть интегрированы в состав *основных* средств ТЗИ.

Информационная безопасность обеспечивается использованием технических средств:

- построения модели защищенной системы;
- управления доступом к ресурсам АС;
- обеспечения целостности и конфиденциальности;
- обеспечения наблюдаемости;
- защиты от воздействий вирусов и иных воздействий, вызывающих любую несанкционированную модификацию информации;
- защиты информации при передаче информации.

Главной задачей технических средств защиты информации является предотвращение умышленного или случайного несанкционированного доступа к информации и ресурсам АС (с целью ознакомления, использования, модификации или уничтожения информации) со стороны авторизованных пользователей или посторонних лиц, которые находятся в пределах зон безопасности информации АС, независимо от способа доступа к этим зонам.

Наиболее значимыми для защиты АС, по мнению авторов, являются *программные средства защиты,* позволяющие создавать модель защищенной автоматизированной системы с построением правил разграничения доступа, централизовано управлять процессами защиты, интегрировать различные механизмы и средства защиты в единую систему, создавать достаточно удобный, интуитивно доступный пользовательский интерфейс администратора безопасности. Причем, с учетом сложности автоматизированной системы, а также необходимости именно комплексного и эффективного использования всех автоматизируемых средств ТЗИ, обеспечения высокой управляемости ими, значительную часть этих средств, по мнению авторов, целесообразно вычленять в достаточно автономную часть АС, в ее специфичную функциональную компоненту или подсистему. *Будем называть эту компоненту Подсистемой защиты информации.*

При этом Подсистема защиты информации, как одна из основных в системе технической защиты информации, должна обеспечивать сохранение основных функциональных свойств защищенных автоматизированных систем (целостности, конфиденциальности, доступности и наблюдаемости) [1].

Оценка способности АС обеспечивать каждое из этих функциональных свойств производится по сформулированной в нормативных документах СТЗИ [2, 3, 4, 5] системе критериев оценки защищенности системы. Состав средств ТЗИ и их вклад в обеспечение функциональных свойств АС могут быть представлены так, как это приведено на рисунке 1.

Как следует из рисунка, подсистема защиты информации обеспечивает решение основных задач обеспечения конфиденциальности, целостности и большинства задач обеспечения наблюдаемости. Средствами же прикладного и базового программного обеспечения решаются некоторые из задач обеспечения конфиденциальности (в части повторного использования объектов), целостности (в части обеспечения отката) и все задачи обеспечения доступности. Средствами ТЗИ телекоммуникаций решаются задачи обеспечения конфиденциальности и целостности в части обмена и обеспечения наблюдаемости в части достоверного канала, идентификации и аутентификации при обмене.

II Подсистема защиты информации

Программные средства защиты (ПСЗ) позволяют создать модель защищенной информационной системы с построением правил разграничения доступа, централизованно управлять процессами защиты, интегрировать различные механизмы и средства защиты в единую систему, создать достаточно удобный для пользователей интерфейс администратора безопасности. Причем, с учетом сложности решения, а также необходимости именно комплексного использования всех автоматизированных средств ТЗИ, их эффективной *управляемости*, значительную часть этих средств целесообразно выделять в достаточно автономную часть АС (специфичный функциональный компонент или подсистему). Будем называть этот компонент *Подсистемой защиты информации* (ПЗИ).

Подсистема защиты информации, как одна из основных функциональных компонент АС, должна обеспечивать решение основных задач обеспечения конфиденциальности, целостности и большинства задач обеспечения наблюдаемости.

Для Подсистем защиты информации, как и для любых других систем подобного уровня сложности, должна применяться компонентная модель построения, суть которой достаточно полно изложена в [11] и заключается в построении системы (программного продукта) из большого количества *независимых* компонент, которые могут разрабатываться отдельно и независимо друг от друга и взаимодействовать только на уровне интерфейсов.

Предлагаемая архитектура Подсистемы защиты информации представлена на рисунке 2. В ее состав, как элементы, входят компоненты (в свою очередь, каждый из компонентов может также состоять из элементов или компонентов), каждый из которых предназначен для реализации определенного набора услуг безопасности и управления. Совокупность таких услуг должна обеспечивать все основные функциональные свойства защищенных АС.

В составе Подсистемы защиты информации целесообразно выделять ее ядро - совокупность компонент, которая реализует основные принципы функционирования и управления Подсистемы защиты информации, правила взаимодействия ее компонент, позволяют гибко конфигурировать состав средств обеспечения защиты в зависимости от динамично изменяющихся условий эксплуатации АС и модели угроз системе. В составе ядра, в свою очередь, можно выделить:

1. Компонент контроля доступа к сервисам Подсистемы защиты информации: реализует функции генерации сеансовых ключей для каждого подключения к серверу Подсистемы защиты информации, контроля полномочий администраторов на выполнение команд управления процессом защиты и ведения базы данных полномочий администраторов.
2. Компонент управления Подсистемой защиты информации: реализует функции управления и контроля за функционированием ядра Подсистемы защиты информации.
3. Компонент управления конфигурацией Подсистемы защиты информации: реализует функцию ведения внутренней базы данных, определяющую текущую структуру активных средств защиты и ключевые параметры их взаимодействия, правил разграничения доступа к ресурсам самой Подсистемы защиты информации, настройки внутренней базы данных параметров функционирования других компонент, реализующих Подсистему защиты информации.
4. Компонент диагностики и тестирования: обеспечивает контроль целостности и, при необходимости, восстановление целостности программных средств самой ПЗИ, а также локализацию ошибок при сбоях и авариях. Обеспечивает тестирование и диагностику при старте системы, при восстановлениях после сбоев и по запросу администратора безопасности.

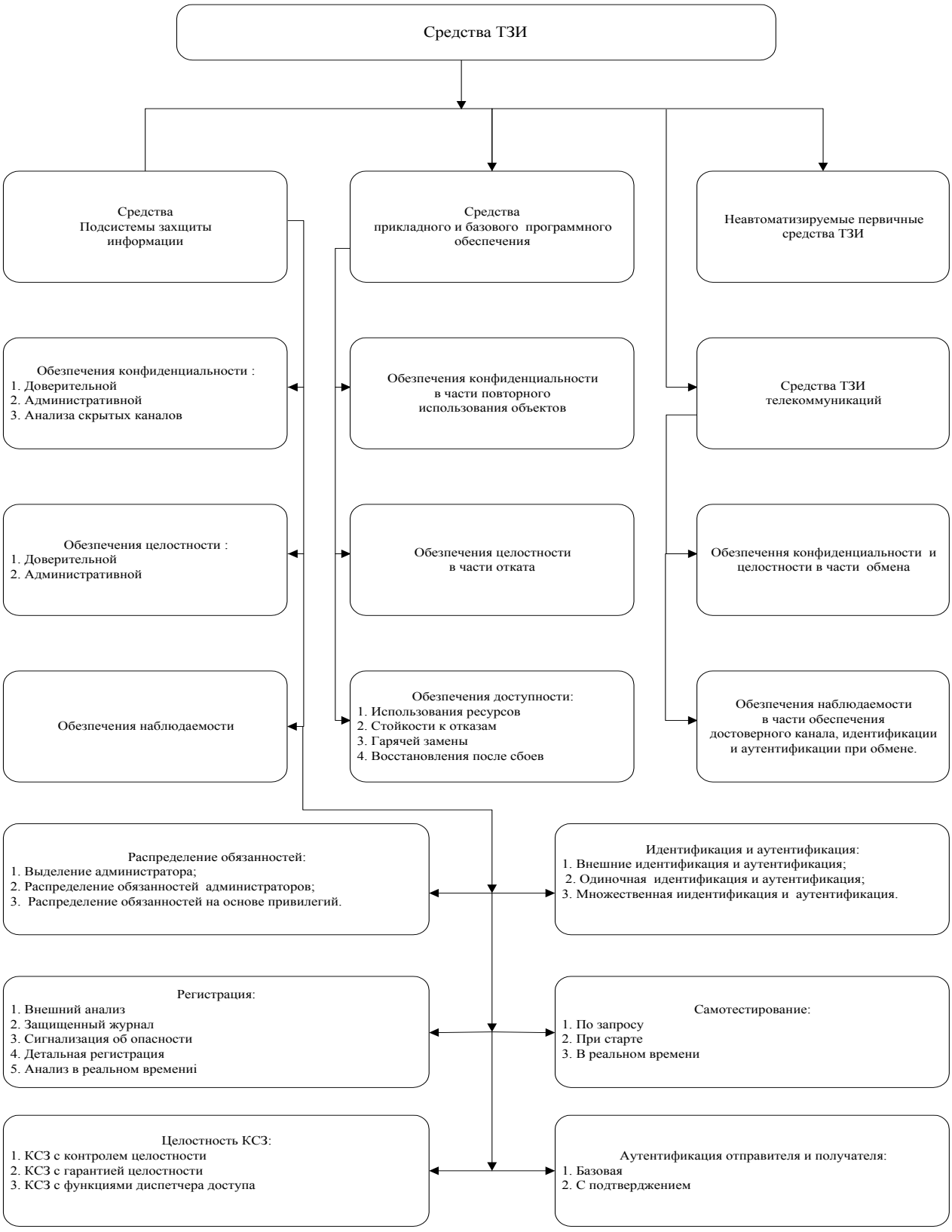

Рисунок 1 – Состав средств ТЗИ и их вклад в обеспечение функциональных свойств АС

5. Компонент управления транзакциями: реализует функции поддержки транзакционной модели выполнения команд ПЗИ, т. е. команда считается выполненной успешно только в том случае, если успешно

выполнены все составляющие ее операции. В случае ошибки ВСЕ результаты выполнения команды должны быть анулированы, система должна быть возвращена в исходное состояние с синхронизацией базы данных модели защищенной системы и реального состояния защищенной системы.

6. Компонент ведения базы данных Подсистемы защиты информации: реализует функции интерпретации команд Подсистемы защиты информации в команды управления данными, поддержки эффективного функционирования базы данных Подсистемы защиты информации (настройка индексов, оптимизация запросов), резервирования и восстановления базы данных Подсистемы защиты информации после сбоев.

7. Компонент обеспечения интерфейсов с внешними средствами защиты: реализует функции установления и поддержки связи с активными компонентами управления средствами контроля физического доступа, управления средствами контроля целостности и криптографической защиты и компонентами управления средствами защиты базового и прикладного программного обеспечения, предоставления сервисов подходящего компонента управления в зависимости от команды, полученной от компоненты построения и реализации модели защищенной системы.

8. Компонент управления взаимодействием с удаленными серверами ПЗИ; предназначен для управления потоком информации между серверами ПЗИ разных уровней (центрального, регионального и местного). Компонент должен реализовывать функции:

- защиты потока информации между серверами ПЗИ разных уровней (в том числе и с использованием криптографических методов);
- синхронизации баз данных ПЗИ разных уровней;
- управления полномочиями администраторов ПЗИ подчиненных уровней.

9. Компонент управления взаимодействием с подсистемами защиты информации посторонних разработчиков: предназначен для управления потоком информации между Подсистемой защиты информации и подсистемами защиты информации других АС при их взаимодействии.

Для централизованного управления подсистемой защиты служат компоненты, обеспечивающие деятельность администраторов Подсистемы защиты информации в составе:

1. Автоматизированного рабочего места (АРМ) администратора Подсистемы защиты информации, которое реализует функции предоставления графического интуитивного интерфейса администратора; выдачи визуальных или звуковых предупреждений о событиях, имеющих критическое влияние на безопасность системы.

2. Компонент взаимодействия с удаленными АРМ Подсистемы защиты информации реализует функции предоставления сервисов Подсистемы защиты информации для удаленного использования, защиты потока информации между компонентами Подсистемы защиты информации и удаленным АРМ (в том числе и с использованием криптографических методов).

3. Компонент взаимодействия с АРМ функциональных подсистем; реализует функции управления потоком информации между Подсистемой защиты информации и АРМ функциональных подсистем, а именно с: АРМ администратора базы данных, АРМ администратора программно-технического комплекса (ПТК), АРМ администратора телекоммуникаций и сетей.

4. Компонент построения и реализации модели защищенной системы; реализует функции: автоматизированного построения модели защищенной системы, т. е. создание структуры объектов, субъектов и правил разграничения доступа в соответствии с выбранной политикой безопасности для данной защищенной системы; ведения классификаторов типов объектов, субъектов, режимов доступа и полномочий субъектов; ведения классификаторов событий. Созданная модель может быть реализована (спроецирована) в защищенной системе вне зависимости от прикладного и базового программного обеспечения, которое используется непосредственно для реализации функций ИС.

5. Компонент контроля состояния защищенной системы; реализует функции: ведения журнала событий, влияющих на состояние безопасности защищенной системы; отслеживания и обработки критичных событий (передача команд на выдачу визуальных и звуковых сообщений АРМ Подсистемы защиты информации, выдача команд на блокирование компонент АС, сигнализирующих о критических событиях и т. д.); предоставление средств управления правилами отслеживания событий для отдельных компонент АС (полный контроль, контроль событий с определенной степенью критичности и т. д.).

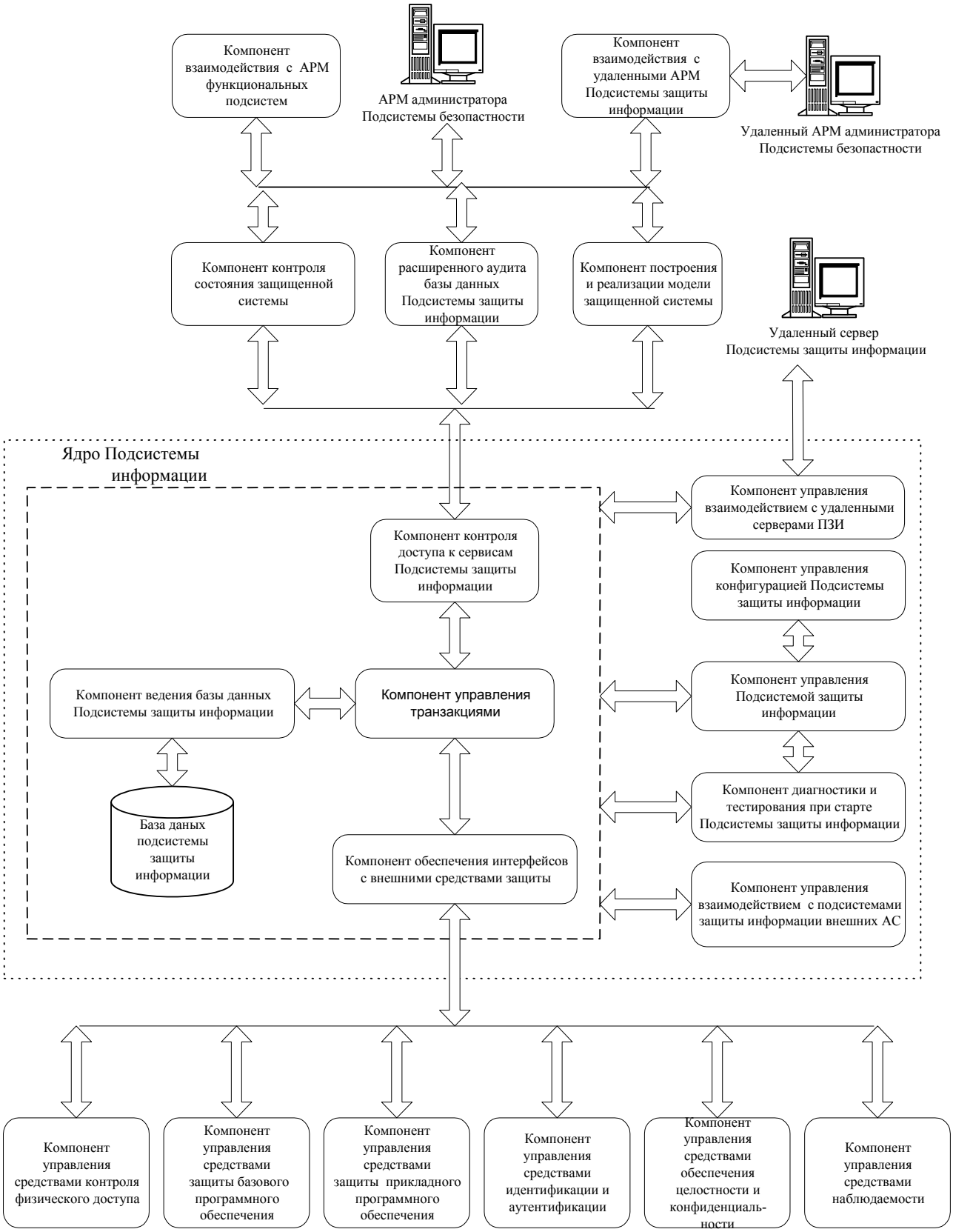

Рисунок 2 - Архитектура Подсистеми защиты информации (ПЗИ)

6. Компонент расширенного аудита базы данных Подсистемы защиты информации; реализует функции: визуального построения и выполнения сложных запросов по базе данных Подсистемы защиты информации (аудит модели системы, аудит журнала событий); представления результатов запросов в удобной для Администратора безопасности форме с выводом результатов на дисплей, принтер или в файл; анализ базы данных Подсистемы защиты информации с применением методов искусственного интеллекта с целью выявления "узких" мест в защите АС.

7. Для реализации услуг и механизмов защиты или управления защищенной системой используются компоненты: Компонент управления средствами контроля физического доступа; реализует функции: интерпретации команд Подсистемы защиты информации в команды управления средствами контроля физического доступа; прием и обработка сообщений о событиях от средств контроля физического доступа.

8. Компонент управления средствами идентификации и аутентификации; реализует функции: управления сервисами идентификации и аутентификации, реализованными в ПЗИ, включая средства идентификации и аутентификации базового или прикладного программного обеспечения АС (NTLMSSP, Kerberos); предоставления сервисов идентификации и аутентификации базовому или прикладному программному обеспечению АС, в случае, если данные сервисы не реализованы или их использование нежелательно (невозможно) по каким-либо причинам.

9. Компонент управления средствами обеспечения целостности и конфиденциальности; реализует функции: управления доступом к ресурсам АС, управления сервисами контроля и восстановления целостности, а также криптографических преобразований, реализованными, в том числе и базовым или прикладным программным обеспечением АС; предоставления сервисов обеспечения целостности и конфиденциальности базовому или прикладному программному обеспечению АС, в случае, если данные сервисы не реализованы или их использование нежелательно (невозможно) по каким либо причинам

10. Компонент управления средствами защиты базового программного обеспечения (при его наличии); реализуют функции: интерпретации команд Подсистемы защиты информации в команды управления средствами защиты базового программного обеспечения; прием и обработку сообщений о событиях от средств защиты базового программного обеспечения.

11. Компонент управления средствами защиты прикладного программного обеспечения; реализует функции: интерпретации команд Подсистемы защиты информации в команды управления средствами защиты прикладного программного обеспечения; прием и обработку сообщений о событиях от средств защиты прикладного программного обеспечения.

12. Компонент управления средствами наблюдаемости обеспечивает управляемость комплексной системой ТЗИ вообще и Подсистемой защиты информации в частности, регистрацию событий, опасных для конфиденциальности и целостности ресурсов АС, собственную целостность и самоконтроль АС.

Предложенная архитектура может служить основой для построения типовых ПЗИ в информационных системах, обеспечивая при этом возможность интеграции различных средств и механизмов защиты с целью обеспечения основных функциональных свойств защищенной системы.

III Заключение

Выделение в составе автоматизированных систем достаточно самостоятельных Подсистем защиты информации унифицированной архитектуры и функций защиты позволит ускорить процесс создания защищенных АС. Это также позволит в дальнейшем обеспечить взаимодействие Подсистем защиты информации при информационном обмене между различными АС.

Литература: 1. Закон України «Про захист інформації в автоматизованих системах» від 05.07.1994 року. 2. ДСТУ 3396.0-96. «Захист інформації. Технічний захист інформації. Основні положення". 3. ДСТУ 3396.1-96. «Захист інформації. Технічний захист інформації. Порядок проведення робіт". 4. ДСТУ 3396.2-97. «Захист інформації. Технічний захист інформації. Терміни та визначення". 5. «Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу» (НД ТЗІ 1.1 – 002 – 99). 6. «Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу» (НД ТЗІ 1.1 – 003 – 99). 7. «Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу» (НД ТЗІ 2.5 – 004 – 99). 8. «Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу» (НД ТЗІ 2.5 – 005 – 99). 9. Положення про порядок здійснення криптографічного захисту інформації в Україні. Утверждено Указом Президента Украини от 22 мая 1998 года № 505/98. 10. Василенко В.С., Короленко М.П. Целостность информации в автоматизированных системах // Корпоративные системы.-1999.-№ 3.-С.52-57. 11. Будько Н.Н., Василенко В.С., Короленко М.П. Архитектура системы защиты информации // Корпоративные системы.-1999.-№ 4.-С.53-57.